

AD-A271 948



June 9, 1982
NUMBER 5400.11



Department of Defense Directive

ASD(C)

2

SUBJECT: Department of Defense Privacy Program

- References:
- (a) DoD Directive 5400.11, "Personal Privacy and Rights of Individuals," August 4, 1975 (hereby canceled)
 - (b) Title 5, United States Code, Section 552a (Public Law 93-579, "The Privacy Act of 1974")
 - (c) DoD 5025.1-M, "Directives System Procedures" April, 1981, authorized by DoD Directive 5025.1, "Department of Defense Directives System," October 16, 1980
 - (d) through (g), see enclosure 1

DTIC
ELECTE
NOV 08 1993
A

A. REISSUANCE AND PURPOSE

1. This Directive reissues reference (a); establishes policies and procedures for implementing the DoD Privacy Program under reference (b); delegates authorities and assigns responsibilities for administration of the DoD Privacy Program; and establishes the Defense Privacy Board and the Defense Privacy Board Legal Committee.

2. This Directive authorizes the development, publication, and maintenance of DoD 5400.11-R, "The DoD Privacy Program Regulation," consistent with reference (c).

B. APPLICABILITY AND SCOPE

1. The provisions of this Directive apply to the Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff, and the Defense Agencies (hereafter referred to as "DoD Components"), except for the National Security Agency/Central Security Service (NSA/CSS) (see subsection B.2., below).

2. This Directive shall apply to the NSA/CSS to the extent that its provisions are consistent with references (d) and (e), and with requirements to protect sensitive cryptologic information.

3. The provisions of this Directive shall be made applicable by contract or other legally binding actions to government contractors whenever a contract is let for the operation of a system of records or a portion of a system of records. For purposes of liability under the Privacy Act (reference (b)) the employees of the contractor are considered employees of the contracting DoD Component.

4. The DoD Privacy Program components are listed at enclosure 2.

93-26809



This document has been approved
for public release and sale; its
distribution is unlimited

93 11 3 052

**Best
Available
Copy**

C. DEFINITIONS

1. Individual. A living citizen of the United States or an alien lawfully admitted to the United States for permanent residence. All members of U.S. Armed Forces are considered individuals for Privacy Act purposes. The legal guardian of an individual or the parent of a minor may act on behalf of the individual. No rights are vested in the representatives of a deceased person under this Directive.

2. Law Enforcement Activity. Any activity engaged in the enforcement of criminal laws, including efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities.

3. System of Records. Any group of records under the control of any DoD Component from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to an individual.

D. POLICY

It is the policy of the Department of Defense to safeguard personal information contained in any system of records maintained by DoD Components and to make that information available to the individual to whom it pertains to the maximum extent practicable.

E. PROCEDURES

Detailed procedures for implementing the DoD Privacy Program are set forth in DoD 5400.11-R. In summary, these procedures:

1. Permit individual access and amendment. Individuals are permitted:
 - a. To determine what records pertaining to them are being collected, maintained, used, or disseminated.
 - b. To gain access to the information pertaining to them maintained in any system of records, and to correct or amend that information.
 - c. To obtain an accounting of all disclosures of the information pertaining to them except when disclosures are made (1) to DoD personnel in the course of their official duties; (2) under DoD 5400.7-R (reference (f)); or (3) to another agency or to an instrumentality of any governmental jurisdiction within or under control of the United States conducting law enforcement activities authorized by law.
 - d. To appeal any refusal to grant access to or amend any record pertaining to them, and to file a statement of disagreement with the record in the event amendment is refused.
2. Limit collection, maintenance, use, and dissemination of personal information. DoD Components are required:

a. To collect, maintain, use, and disseminate personal information only when it is relevant and necessary to achieve a purpose required by statute or Executive Order.

b. To collect personal information directly from the individuals to whom it pertains to the greatest extent practical.

c. To inform individuals who are asked to supply personal information for inclusion in any system of records:

- (1) The authority for the solicitation;
- (2) Whether furnishing the information is mandatory or voluntary;
- (3) The intended uses of the information;
- (4) The routine disclosures of the information that may be made outside the Department of Defense; and
- (5) The effect on the individual of not providing all or any part of the requested information.

d. To ensure that all records used in making determinations about individuals are accurate, relevant, timely, and complete.

e. To make reasonable efforts to ensure that records containing personal information are accurate, relevant, timely, and complete for the purposes for which the record is being maintained before making them available to any recipients outside the Department of Defense, other than a federal agency, unless the disclosure is made under DoD 5400.7-R (reference (f)).

f. To keep no record that describes how individuals exercise their rights guaranteed by the First Amendment of the U.S. Constitution, unless expressly authorized by statute or by the individual to whom the records pertains, or the record is pertinent to and within the scope of an authorized law enforcement activity.

g. To make reasonable efforts, when appropriate, to notify individuals whenever records pertaining to them are made available under compulsory legal process, if such process is a matter of public record.

h. To establish safeguards to ensure the security of personal information and to protect this information from threats or hazards that might result in substantial harm, embarrassment, inconvenience, or unfairness to the individual.

i. To establish rules of conduct for DoD personnel involved in the design, development, operation, or maintenance of any system of records and to train them in these rules of conduct.

3. Require public notice and annual publication. DoD Components are required to publish in the Federal Register:

- a. At least annually, a notice of the existence and character of every system of records maintained.
 - b. A notice of the establishment of any new or any alteration to existing system of record notices.
 - c. At least 30 days before adoption, advance notice for public comment of any new or intended changes to the routine uses of the information in existing system of records including the categories of users and the purposes of such use.
4. Permit exempting eligible systems of records. DoD Components may exempt from certain specific provisions of the Privacy Act (reference (b)) eligible systems of records, but only when there is an important public purpose to be served and specific statutory authority for the exemption exists.
 5. May require annual and other reports. DoD Components shall furnish the Privacy Office that information required to complete any reports required by the Office of Management and Budget or other authorities.

F. ORGANIZATION

1. Defense Privacy Board. Membership of the board shall consist of the Executive Secretary and representatives designated by the Secretaries of the Military Departments; the Assistant Secretary of Defense (Comptroller) (whose designee shall serve as chairman); the Assistant Secretary of Defense (Manpower, Reserve Affairs, and Logistics); the General Counsel, Department of Defense; and the Director, Defense Logistics Agency;
2. The Defense Privacy Office. The office consists of a Director, who shall also function as the Executive Secretary of the Defense Privacy Board, and his staff.
3. The Defense Privacy Board Legal Committee. The committee shall be composed of a legal counsel from each of the DoD Components represented on the DoD Privacy Board. The legal counsels shall be appointed by the Executive Secretary in coordination with the Secretaries of the Military Department or the head of the appropriate DoD Components. Other DoD legal counsels may be appointed by the Executive Secretary, after coordination with the appropriate representative of the DoD Component concerned, to serve on the committee.

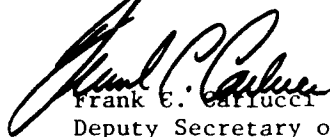
G. RESPONSIBILITIES

1. The Assistant Secretary of Defense (Comptroller) (ASD(C)), or his designee, the Deputy Assistant Secretary of Defense (Administration) (DASD(A)), shall:
 - a. Direct and administer the DoD Privacy Program.
 - b. Develop and maintain DoD 5400.11-R consistent with DoD 5025.1-M (reference (c)), and other guidance, to ensure timely and uniform implementation of the DoD Privacy Program.
 - c. Serve as chairman of the Defense Privacy Board.

2. Chairman and members of the Defense Privacy Board shall:
 - a. Serve as the principal policymakers for the DoD Privacy Program and the focal point for implementation of this Directive.
 - b. Ensure that all DoD Components actively participate in establishing policies, procedures, and practices in carrying out the DoD Privacy Program.
3. Director, Defense Privacy Office, shall carry out the specific responsibilities for implementation of the DoD Privacy Program set forth in enclosure 3.
4. Members of Defense Privacy Board Legal Committee shall:
 - a. Consider legal questions referred to the Board regarding the application of the Privacy Act (reference (b)), this Directive, DoD 5400.11-R, and the implementation of the DoD Privacy Program.
 - b. Render advisory opinions to the DoD Privacy Board, subject to approval by the General Counsel, Department of Defense.
5. The General Counsel, Department of Defense, shall:
 - a. Review the advisory opinions of the Defense Privacy Board Legal Committee to ensure uniformity in legal positions and interpretations rendered.
 - b. Be the final approving authority on all advisory legal opinions rendered by the Defense Privacy Board or the Defense Privacy Board Legal Committee regarding the Privacy Act (reference (b)) or its implementation.
6. The Head of Each DoD Component shall implement the DoD Privacy program by carrying out the specific responsibilities set forth in subsection E.2. and enclosure 4.
7. System Managers shall carry out the responsibilities set forth in enclosure 5.
8. Automated Data Processing (ADP) or Word Processing Managers, who process information from any system of records, shall carry out the responsibilities set forth in enclosure 6.
9. DoD Employees shall:
 - a. Not disclose any personal information contained in any system of records except as authorized by this Directive.
 - b. Not maintain any official files which are retrievable by name or other personal identifier without first ensuring that a notice for the system has been published in the Federal Register.
 - c. Report any disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized by this Directive to the appropriate Privacy Act officials for his or her action.

H. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Although DoD 5400.11-R expands on this Directive and implements the DoD Privacy Act Program, DoD Components shall forward within 180 days two copies of their internal implementing documents to the Assistant Secretary of Defense (Comptroller) to ensure compliance with paragraph G.2.b. of the basic Directive, and paragraph 5, enclosure 3.



Frank E. Carlucci

Deputy Secretary of Defense

Enclosures - 6

1. References
2. DoD Privacy Program Components
3. Responsibilities of the Director, Defense Privacy Office
4. Responsibilities of DoD Component Heads
5. Responsibilities of the System Manager
6. Responsibilities of ADP and Word Processing Managers

Jun 9, 82
5400.11 (Encl 1)

REFERENCES (continued)

- (d) Public Law 86-36, "National Security Agency," May 29, 1959
- (e) Public Law 88-290, "Personnel Security Procedures in the National Security Agency," March 26, 1964
- (f) DoD 5400.7-R "DoD Freedom of Information Act Program," December 1980, authorized by DoD Directive 5400.7, "DoD Freedom of Information Act Program," March 24, 1980
- (g) Title 12, United States Code, Section 3401, "The Financial Privacy Act of 1978"

Accession For	
NTIS CRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By <i>from 50</i>	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
<i>A-1</i>	

DOD PRIVACY PROGRAM COMPONENTS

Office of the Secretary of Defense and its field activities
Department of the Army
Department of the Navy
Department of the Air Force
U.S. Marine Corps
Organization of the Joint Chiefs of Staff
Unified and Specified Commands
Defense Advanced Research Projects Agency
Defense Audiovisual Agency
Defense Audit Service
Defense Communications Agency
Defense Contract Audit Agency
Defense Criminal Investigative Service
Defense Intelligence Agency
Defense Investigative Service
Defense Logistics Agency
Defense Mapping Agency
Defense Nuclear Agency
Defense Security Assistance Agency
National Security Agency/Central Security Service
Uniformed Services University of the Health Sciences

RESPONSIBILITIES OF THE DIRECTOR, DEFENSE PRIVACY OFFICE

The Director, Defense Privacy Office, shall:

1. Serve as Executive Secretary and a member of the Defense Privacy Board.
2. Monitor implementation of the DoD Privacy Program for the Defense Privacy Board.
3. Serve as the focal point for the coordination of Privacy Act matters with the Defense Privacy Board; the Defense Privacy Board Legal Committee; the Office of Management and Budget; the General Accounting Office; the Office of the Federal Register, in conjunction with the OSD Federal Register Liaison Officer; and other federal agencies, as required;
4. Develop and maintain DoD 5400.11-R consistent with DoD 5025.1-M reference (c)).
5. Review DoD Component instructions and related issuances pertaining to the DoD Privacy Program and provide overall guidance to avoid conflict with DoD Privacy Program policy and procedures.
6. Supervise the implementation of the Right to Financial Privacy Act of 1978 (reference (g)) and any other legislation that impacts directly on individual privacy.
7. In conjunction with the Office of the Assistant Secretary of Defense (Manpower, Reserve Affairs, and Logistics), the Office of the General Counsel, DoD; and other DoD Components:
 - (a) Ensure that training programs regarding DoD Privacy Program policies and procedures are established for all DoD personnel whose duties involve design, development, operation, and maintenance of any system of records.
 - (b) Coordinate on all DoD personnel policies that may affect the DoD Privacy Program.
8. In conjunction with the Office of the Deputy Assistant Secretary of Defense (Management Systems), Office of the ASD(C), and other DoD Components, ensure that:
 - (a) All information requirements developed to collect or maintain personal data conform with DoD Privacy Program standards;
 - (b) Procedures are developed to protect personal information while it is being processed or stored in automated data processing or word processing centers.
9. In conjunction with the Office of the ASD(MRA&L), the Defense Manpower Data Center (Defense Logistics Agency), and other DoD Components, ensure that procedures developed to collect or maintain personal data for research purposes conform both to the requirements of the research and DoD Privacy Program standards.

RESPONSIBILITIES OF DOD COMPONENT HEADS

The Head of each DoD Component shall:

1. Establish an active program to implement the DoD Privacy Program.
2. Provide adequate funds and personnel to support the Privacy Program.
3. Designate a senior official to serve as the principal point of contact for DoD Privacy Program matters and to monitor compliance with the program.
4. Ensure that DoD Privacy Program compliance is reviewed during the internal inspections conducted by Inspectors General or equivalent inspectors.
5. Ensure that the DoD Component head, a designee, or an appellant reviews all appeals from denials or refusals by Component officials to amend personal records.
6. Establish rules of conduct to ensure that:
 - a. Only personal information that is relevant and necessary to achieve a purpose required by statute or Executive Order is collected, maintained, used, or disseminated.
 - b. Personal information is collected to the greatest extent practicable directly from the individual to whom it pertains.
 - c. No records are maintained describing how individuals exercise their rights guaranteed by the First Amendment to the U.S. Constitution unless expressly authorized by statute or the individuals to whom they pertain or unless the records pertain to and are within the scope of an authorized law enforcement activity.
 - d. Individuals are granted access to records which pertain to them in systems of records unless the system has been exempted from the access provisions of the Privacy Act (reference (b)).
 - e. No system of records subject to reference (b) is maintained, used, or disseminated without prior publication of a system notice in the Federal Register.
 - f. All personal information contained in any system of records is safeguarded against unwarranted and unauthorized disclosure.
 - g. Procedures are established that permit an individual to seek the correction or amendment of any record in a system of records pertaining to the individual unless the system of records has been exempted from the amendment procedures of reference (b).
 - h. All personnel whose duties involve design, development, operation, and maintenance of any system of records are trained in the rules of conduct established.

Jun 9, 82
DoD 5400.11 (Encl 4)

7. Assist, upon request, the Defense Privacy Board on matters of special interest.

RESPONSIBILITIES OF THE SYSTEM MANAGER

The System Manager for any system of records shall:

1. Ensure that all personnel who either have access to the system of record or who are engaged in developing or supervising procedures for handling records in the system of records are aware of their responsibilities for protecting personal information established by the DoD Privacy Program.
2. Prepare promptly any required new, amended, or altered system notices for the system of records and submit them through channels for publication in the Federal Register.
3. Notify all ADP or word processing managers who process information from the system of records that the information is subject to the DoD Privacy Program and the applicable routine uses for the information in the system.
4. Coordinate with ADP and word processing managers providing services to ensure an adequate risk analysis is conducted.
5. Coordinate with the servicing ADP and word processing managers to ensure that the system manager is notified when there are changes to processing equipment, hardware or software, and the data base that may require submission of a amended system notice.

RESPONSIBILITIES OF ADP AND WORD PROCESSING MANAGERS

All ADP and word processing managers, who process information from a system of records shall:

1. Ensure that each system manager provides a current system notice or information as to the contents of the system notice for each system of records from which information is to be processed.
2. Ensure that all personnel who have access to information from a system of records during processing or who are engaged in developing procedures for processing such information are aware of the provisions of the DoD Privacy Program policies and procedures.
3. Notify promptly the system manager whenever there are changes to processing equipment, hardware or software, and the data base that may require the submission of an amended system notice for any system of records.